IDEA GROUP PUBLISHING

701 E. Chocolate Avenue, Suite 200, Hershey PA 17033-1240, USA **ITB9466**
Tel: 717/533-8845; Fax 717/533-8661; URL-http://www.idea-group.com

Chapter XIV

Ethics and Digital Government

Ronald E. Anderson
University of Minnesota, USA

ABSTRACT

After considering the high costs to digital government of inadequate ethical choices, the role of ethics in government generally is reviewed. While codes of ethics may not go far toward resolving ethical challenges, they provide bases for ethical discourses and embody key ethical principles. Selected principles from the Code of Ethics of the Association for Computing Machinery (ACM) are applied to contemporary ethical issues in the context of digital government. In the rapidly evolving environments of digital technology, it is impossible to anticipate the leading-edge ethical issues. However, there are solid ethical or moral imperatives to use these principles for resolution of the issues.

ETHICS AND THE COST OF DIGITAL GOVERNMENT

Inadequate ethical decision-making results in major cost implications for digital government. One cost area is unauthorized system access, particularly for producing damage, e.g., from computer code commonly called viruses. The other problem area is that of poor system design, particularly software failing to meet professional standards of

quality. The former generally results from persons with an ethically defective intent to produce harm to the systems and their users. The latter generally results from the neglect of professional ethical standards requiring the implementation of a quality development process that yields quality products.

Security Failures

In the 1970s, when researchers first began to study the impact of information technology (IT) upon municipal and federal governments, their discourse rarely contained the terminology of risks, vulnerability or even unauthorized access (Kraemer, 1976). Even 20 years later, as the Internet began to play major roles in business and government, security breaches in IT systems generally were not seen as grave problems. Now, despite the regular practice of anti-virus screening and related procedures, security problems are expected and treated with utmost seriousness. Solutions are no longer seen as solely technical but social and ethical as well. Typically the IT (information technology) or IS (information system) departments in government agencies establish complex procedures allowing access to different system resources only by specific categories of employees. In addition, these agencies typically establish codes of conduct and require employees to sign an acceptable use policy (AUP).

Despite these ethics-related measures to contain malicious attempts to violating information systems, there are millions of destructive agents circulating the Internet at any given moment. In the year 2000, *InformationWeek* Research and PricewaterhouseCoopers LLP jointly conducted a global survey of 4,900 IT professionals across 30 nations to help estimate the cost of viruses and computer hacking.[1] The study estimated that the one-year cost amounted to more than 2.5% of the United States' Gross Domestic Product (GDP). Furthermore, the estimate cost worldwide was $1.6 trillion for the year 2000.

Quality Control Failures

Breakdowns in hardware are well known but software malfunctions are far more elusive. System failures are inherent to large software systems due to their complexity. Malfunctions also occur from design and programming mistakes, from errors in data input, and from user errors. Peter Neumann (1995) has devoted much of his professional career over the past two decades to documenting system risks and has found that a large share of them are due to failures in quality control. He continues to manage an Internet forum "The Risks Digest — Forum on Risks to the Public in Computers and Related Systems."[2] Many of his collected stories reveal the huge cost of system malfunctions that could have been avoided if professional standards of quality control had been followed. The ethical standards of the Software Engineering Society (Gotterbarn, 1991) as well as the Association for Computing Machinery (ACM) specify professional responsibility to follow quality processes and ensure quality systems.[3] Digital government systems, especially in the areas of revenue management and tax collection, with inherent weaknesses due to poor construction quality may yield huge financial costs.

Non-Monetary Costs

Failure to comply with IT-related ethical standards may result in major non-monetary losses such as the loss of personal privacy. Digital government systems for